vtServer®

vtAlpha/vtVAX Bare Metal

V4.0.0

vtServer Cloud Setup Guidelines

Technical Note

BN-0015-03

vtServer Cloud Setup Guidelines

BN-0015-03 (April 8, 2019)

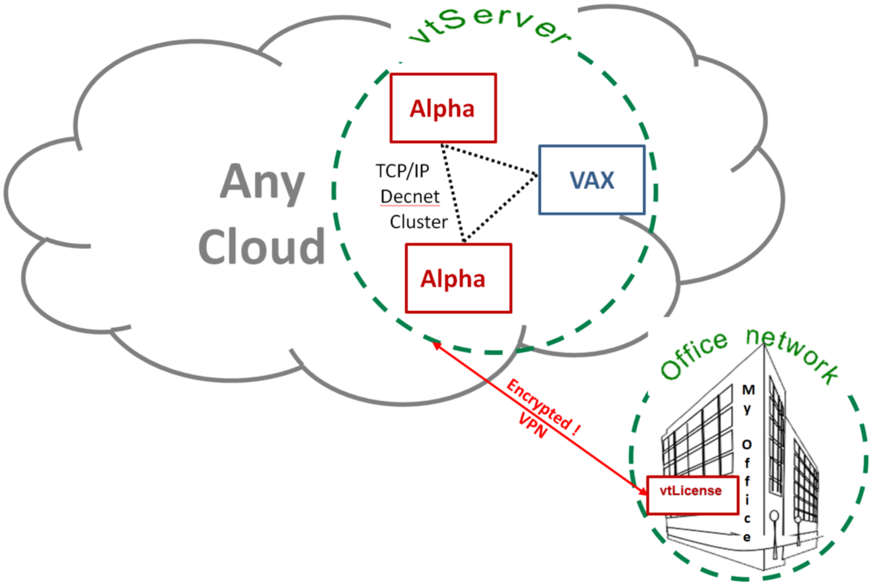
vtAlpha and vtVAX are marketed jointly by AVT and Vere Technologies LLC

Table of Contents

1. Introduction

Until recently DEC Alpha and VAX users had two choices: Continue to run on the legacy hardware, or use emulation to run a 'virtual' Alpha or VAX on a PC server. Now with the latest vtServer product from AVTware, it is easy to run an OpenVMS or Tru64 server in the Cloud – free of the responsibility to install or maintain any hardware. This new version of vtServer is called vtCloud.

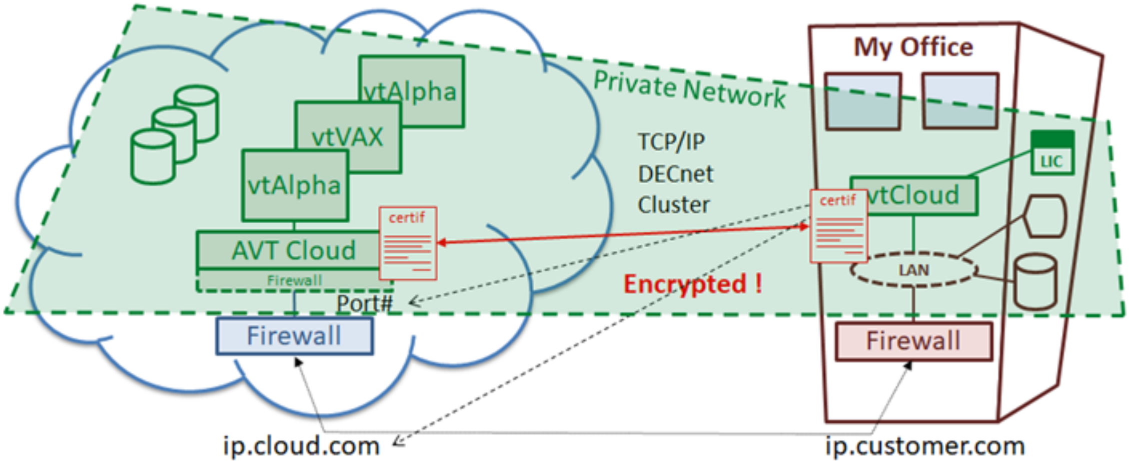
The Cloud began as a metaphor for the Internet, but now it is synonymous with the ability to run applications and data anywhere on the Internet as if they are still in your office. Cloud companies provide all the hardware resources your applications require. Now VSI and AVT provide the remote installation, provisioning and monitoring of your applications in the Cloud as if they are still running in your local office, but the Alpha or VAX system in the Cloud can be located anywhere on earth.



vtCloud includes a secure and transparent VPN tunnel from the Cloud provider to your office for the highest security. From the end user's perspective, there is no functional difference between vtServer emulating an Alpha system in the Cloud and vtServer emulating an Alpha system in the office. In either scenario, it is possible to create stand-alone systems and/or OpenVMS clusters, and the cluster members can be located at any Cloud provider available.

Shadow disks can be placed thousands of miles from each other. Failover systems can be placed anywhere, even in another part of the world.

The connection from vtCloud to the local network is secure and transparent. vtCloud has its own firewall and the local network is only available via VPN connection. The VPN connection is encrypted and uses unique generated security keys to ensure maximum security.

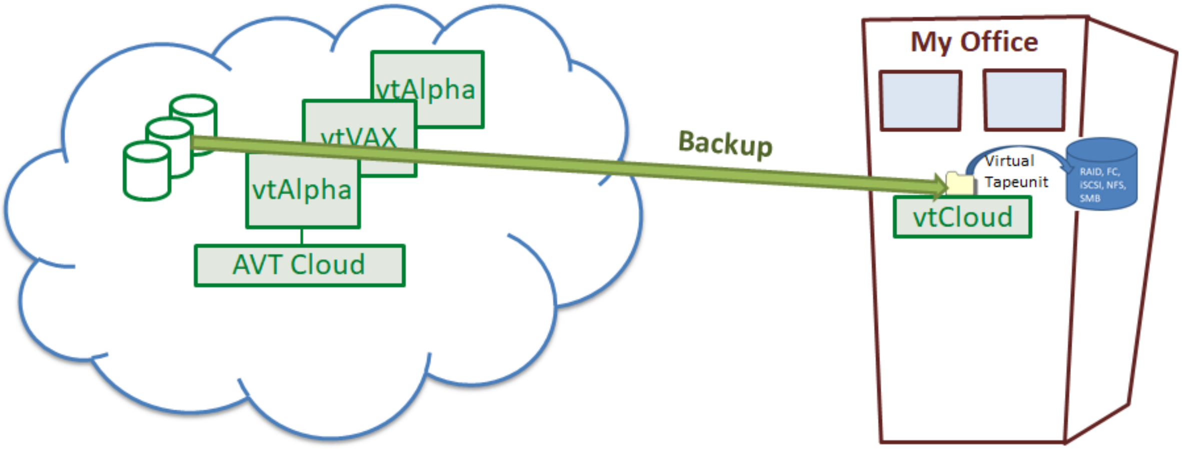


The VPN connection between vtCloud and the local network supports all network protocols used in an Alpha or VAX environment. The servers in vtCloud can be used as if they are in the local network.

All network protocols are supported so the servers will behave the same as if they were on the local network:

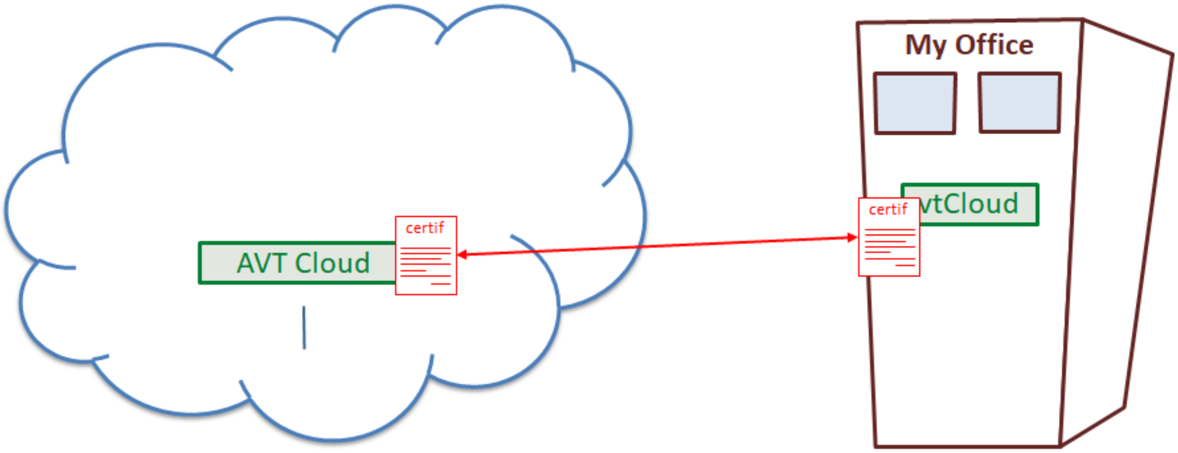
- OpenVMS cluster
- DECnet traffic
- MOP boot
- OpenVMS disk shadowing
- NFS and SMB mounts
- TCP/IP traffic
- Virtual tape units in the office, used by servers in vtCloud
- iSCSI devices
- Fibre Channel connections
- Etc.

Backups from data located in vtCloud can be made on virtual tape units, or copied to network disks (NFS, SMB) located in the local network.



The connection from your local network to vtCloud is setup via a vtLicense server that is available from AVT, VERE or one of their resellers. This vtLicense server takes care of the encrypted VPN tunnel, provides the vtLicense key(s) and acts as a bridge between the Cloud and the office. The vtLicense server and the license keys are located on your local network to enhance security.

To ensure a safe connection, individually generated security keys are used to encrypt the VPN connection.



1.1. The Cloud

There is not ONE Cloud.

Several Cloud implementations are available, each with their own functionalities and advantages.

Cloud providers don’t run straight Windows or Linux. They use a ‘software stack’ that includes a hypervisor that allows them to address different models of the underlying hardware in a uniform way.

The first decision is a choice between an open source implementation and a vendor-specific Cloud.

The advantage of an open source Cloud provider is that it is easy to switch to another vendor, because of the common software stack. Only small changes should be enough to make it work when you switch to another open source provider. The most commonly used non-proprietary open source Cloud software is OpenStack. OpenStack does not have its own hypervisor but can utilize different hypervisors, such as KVM, Xen and ESXi.

When using a vendor-specific Cloud, moving to a different Cloud provider can be more complicated, because of underlying differences in Cloud architecture.

For example, Microsoft Cloud uses Azure, which is an extension of Microsoft's Hyper-V hypervisor:

https://www.networkworld.com/article/3037483/cloud-computing/truly-understanding-microsoft-s-azure-stack.html

The Azure Stack is running Microsoft’s Hyper-V, Windows, and Microsoft networking and storage, but the end user doesn’t see any of that. However, if you start with Azure stack, then you have to stay with Azure, or prepare for a complex conversion.

In addition to Azure, a few well-known Cloud providers are:

Amazon	AWS (Amazon Web Services)
Oracle	Oracle Cloud
Google	Google Cloud

vtServer /our emulators support any of these Cloud solutions. If you have not already selected a Cloud provider, AVT, VERE or your value-added reseller (VAR) can assist you in deciding which option best meets your IT requirements. For further information regarding hypervisors, please refer to our Technical Note:

http://www.vax-alpha-emulation.com/documents/BN-0001-04_tech_note_vtserver_hypervisor.pdf

For further details on how to use vtCloud on specific Cloud providers, please refer to our documents as follows:

BN-0016 Cloud Setup: H4Y

BN-0017 Cloud Setup: Oracle

BN-0018 Cloud Setup: AWS

2. Cloud Configuration

When running vtCloud (vtServer in the Cloud) it needs a Compute Instance. A compute instance is a virtual machine (VM) that exists in the Cloud, having CPU, memory, storage and network connectivity. To make vtServer work in the Cloud, the following is needed:

1. A compute instance with CPU, memory, storage, and an IP address with access to the Internet. A Cloud provider will provide these components.
2. A dedicated vtLicense server connected to the customer's network and connected to the Internet. This vtLicense server is provided by AVTware and it is the gateway/bridge between the Cloud and the local network.

When vtServer is installed on the compute instance, the "Cloud setup" menu option (found in the console menu) must be executed to create a VPN connection between vtServer running at the Cloud provider and the vtLicense server in your office.

Similarly the Cloud setup must be performed on the vtLicense server.

The easiest workflow is to setup vtServer in the Cloud first, and configure vtLicense as the next step, although this has no effect on the working of vtCloud.

This document guides you through this vtCloud configuration process.

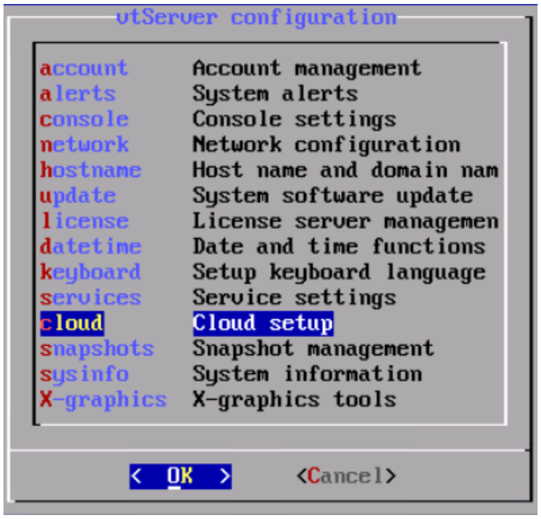
2.1. vtServer Configuration

Before starting the Cloud configuration, be sure to get the following information. It is needed to complete the Cloud configuration.

1. The port number for the VPN connection.
2. The external IP address given to the compute instance.

The Cloud setup can only be executed using the vtServer console menu.

Login on the vtServer console and go to the "**vtServer Configuration"**

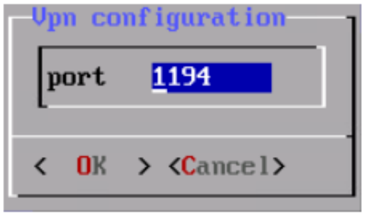


```
vtServer configuration
account     Account management
alerts      System alerts
console     Console settings
network     Network configuration
hostname    Host name and domain nam
update      System software update
license     License server managemen
datetime    Date and time functions
keyboard    Setup keyboard language
services    Service settings
cloud       Cloud setup
snapshots   Snapshot management
sysinfo     System information
X-graphics  X-graphics tools

      <  OK  >      <Cancel>
```

Continue with "**Create**" Create cloud config**" (Create option not shown)**

Read the notice and continue with **Yes**.



```
Vpn configuration
port     1194

<  OK  > <Cancel>
```

Enter the port number to use for the VPN.

The port number is the port used to setup the VPN link to vtServer in the Cloud.

The port number can be any number between 1024 and 65535. The only restriction is that it is free to use on the current network.

The default VPN port number is 1194.

> Remember the port number. It is needed to setup a VPN to this cloud instance on the vtLicense server.

The vtServer setup continues with the setup of the Cloud Management port CLM0. This interface is used to create a VPN between vtServer in the Cloud and vtLicense.

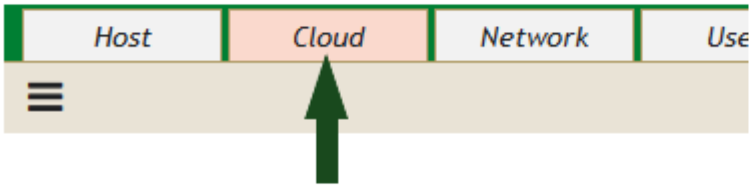
IP DHCP client functionality can be used to get an IP address for the Cloud management port.

For the external Internet port eth0, the IP address given by the Cloud provider must be used.

This address is also needed in the VPN configuration on the vtLicense server.

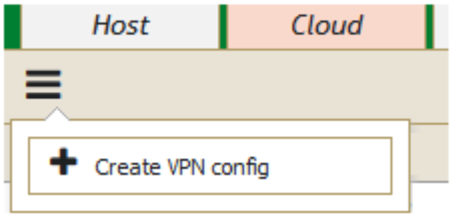
2.2. vtLicense Configuration

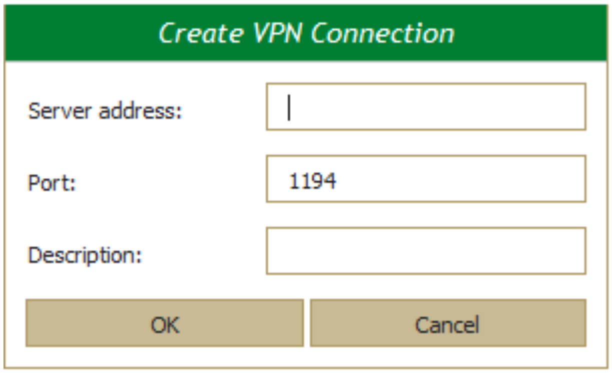
Login into the vtLicense server and select the menu option Cloud.



A license server can establish a VPN to more than one vtServer in the Cloud.

To setup a new VPN select the in cloud sub-menu “Create VPN config”, otherwise select the VPN you want to manage.





Create VPN Connection

Server address:

Port: 1194

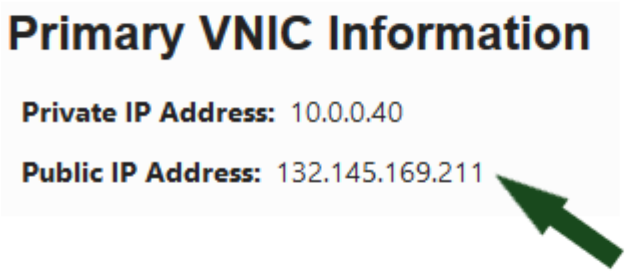
Description:

The server address is the Internet IP address of the vtServer in the Cloud

This IP address is provided by the Cloud provider and is often called the Public IP Address.

Example:

When using Oracle Cloud the Public IP Address is shown as part of the detailed view for an Instance.



Primary VNIC Information

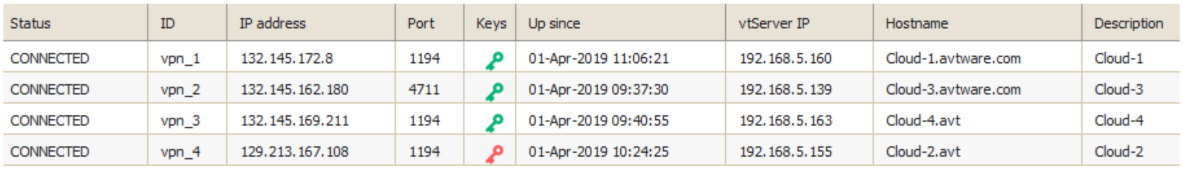
Private IP Address: 10.0.0.40

Public IP Address: 132.145.169.211

The port number must be the same as used in the vtServer Cloud setup.

The description is used to differentiate the VPNs.

The vtLicense server will now create a VPN connection with the vtServer in the Cloud, so that the vtServer in the Cloud will become part of the local network. The vtServer in the Cloud is now accessible on your local network.



Status	ID	IP address	Port	Keys	Up since	vtServer IP	Hostname	Description
CONNECTED	vpn_1	132.145.172.8	1194	🔑	01-Apr-2019 11:06:21	192.168.5.160	Cloud-1.avtware.com	Cloud-1
CONNECTED	vpn_2	132.145.162.180	4711	🔑	01-Apr-2019 09:37:30	192.168.5.139	Cloud-3.avtware.com	Cloud-3
CONNECTED	vpn_3	132.145.169.211	1194	🔑	01-Apr-2019 09:40:55	192.168.5.163	Cloud-4.avt	Cloud-4
CONNECTED	vpn_4	129.213.167.108	1194	🔑	01-Apr-2019 10:24:25	192.168.5.155	Cloud-2.avt	Cloud-2

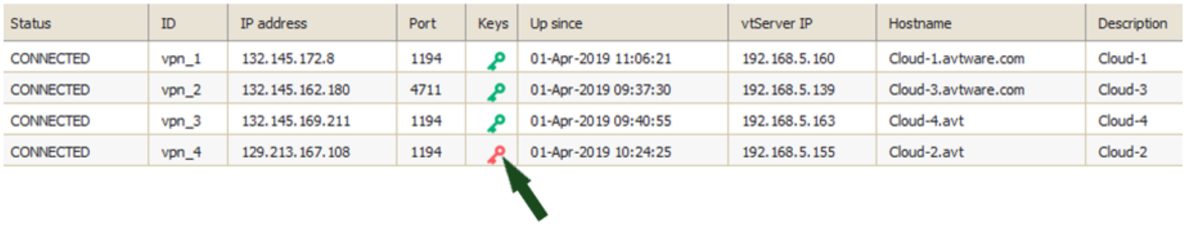
After the VPN is set up, you can connect to the IP address that is set on the cloud management port clm0 on the vtServer in the Cloud.

2.3. VPN Security Keys

When the VPN is created, default security keys are used.

Security keys are used to make the connection secure and not accessible by other processes. The default security keys are the same for all vtCloud VPN connections.

A VPN using the default key is seen with a red key in the cloud window.



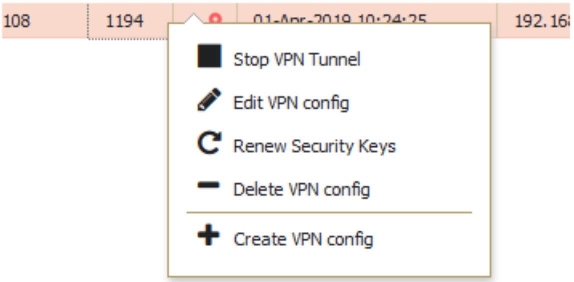
Status	ID	IP address	Port	Keys	Up since	vtServer IP	Hostname	Description
CONNECTED	vpn_1	132.145.172.8	1194	🟩	01-Apr-2019 11:06:21	192.168.5.160	Cloud-1.avtware.com	Cloud-1
CONNECTED	vpn_2	132.145.162.180	4711	🟩	01-Apr-2019 09:37:30	192.168.5.139	Cloud-3.avtware.com	Cloud-3
CONNECTED	vpn_3	132.145.169.211	1194	🟩	01-Apr-2019 09:40:55	192.168.5.163	Cloud-4.avt	Cloud-4
CONNECTED	vpn_4	129.213.167.108	1194	🟥	01-Apr-2019 10:24:25	192.168.5.155	Cloud-2.avt	Cloud-2

A VPN using a secure key is seen with a green key in the cloud window.

To make the VPN more secure, it is advisable to generate unique keys to use for the VPN. These keys are created on the vtLicense server at request and copied to the vtServer in the Cloud. Because these keys are generated specially for the current VPN connection, these keys are unique and make the VPN connection very secure.

Before generating unique security keys, the system time on the vtServer and vtLicense installation must be the same. When the system times are not the same, the new keys will not work immediately.

To generate unique security keys right-click on the VPN to be updated to get a pulldown menu with several options.



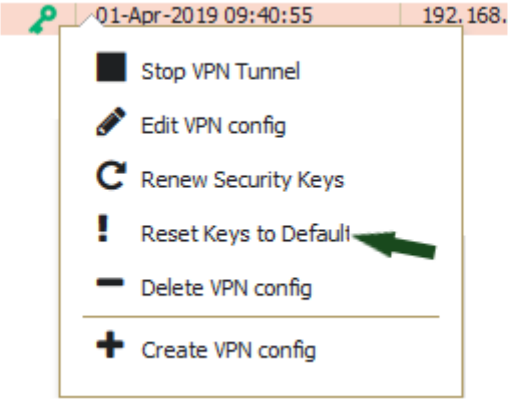
Stop VPN Tunnel	To stop the VPN connection; when the VPN connection is stopped this option will show Start VPN Tunnel
Edit VPN config	To modify the VPN description
Renew Security Keys	Renew the security keys
Delete VPN config	Delete the whole VPN configuration
Create VPN config	Create a new VPN configuration

To renew the keys, the current VPN needs to be stopped and started to use the new keys. In most cases this is done in a short time and the network connections that make use of the VPN are not interrupted. Despite this, it is advisable to minimize the use of the VPN during the renewal of the keys.

To use the Renew Security Keys option, the root password must be the same on the vtCloud server and the vtLicense server.

If the passwords are not the same, a renewal of the keys can only be done via the console menu.

To restore the default keys, the option Reset Keys to Default is present when secure keys are in use.



2.4. Prepare vtServer for the Cloud

In most Cloud environments, a special vtServer image must be uploaded.

If possible, it is practical to configure this image before uploading.

Consider the following settings:

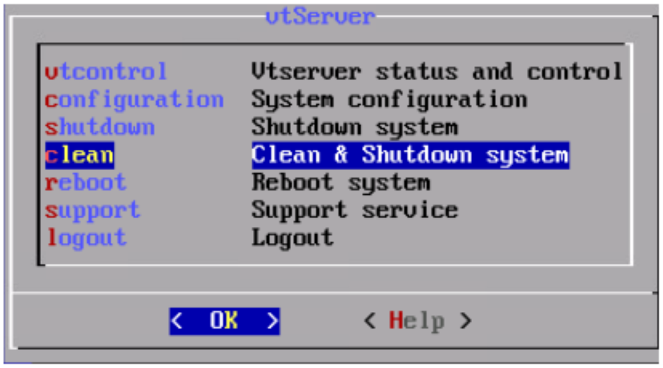
1. The vtServer often has to be installed with an additional installation option.
   Example: serialconsole = ttyS0 for Oracle Cloud.
2. When the Cloud Setup is performed, a number of choices must be made:
   - The VPN port number
   - The IP address choices for the clm0 and eth0 ports

     Eth0 gets its IP address from the Cloud provider, often via DHCP; then choose DHCP enabled for eth0.

     The IP address for clm0 is an IP address within the local network; enter the desired address here or choose DHCP if DHCP is used in the local network.

3. To further complete the configuration of the vtServer, a number of services can be activated. Think in particular of SSH.

Before an "image" can be made of this vtServer installation, it is important to reset a number of settings. This can be done with the "Clean" shutdown option.



From this vtServer installation an "image" can be created that can be uploaded to the Cloud. Because every Cloud provider sets its own requirements for the image, this is not addressed further here.

A separate document is available for the following Cloud environments:

Oracle
Amazon Web Services (AWS)
Host for Yourself (H4Y)

AVTware can provide a pre-configured image, ready to upload to the Cloud.

This pre-configured image has default settings for the port number and IP address configuration.

VPN port number:	1194
IP configuration clm0	DHCP enabled
IP configuration eth0	DHCP enabled

When this image is uploaded to the Cloud and an instance is made using this image, there may be a need to connect to this image to customize these settings.

Therefore an extra option is built into a Cloud image, i.e., a special SSH connection for first time configurations.

2.4.1. SSH Access to Cloud Instance

Immediately after starting it is possible to log in to vtServer without using the VPN connection.

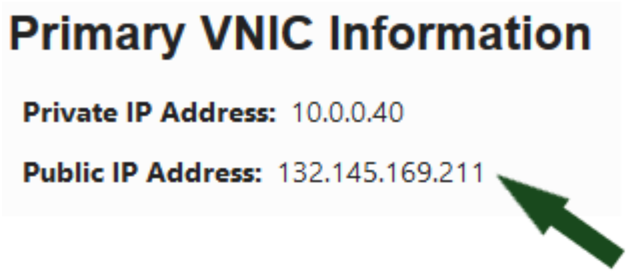
This connection is only available for 15 minutes and is then stopped automatically.

This special connection is only intended for use to adjust the Cloud configuration of vtServer if there is no VPN connection with the vtLicense server. If there is a VPN connection with a vtLicense server, and if the vtCloud server has a local IP address, this extra connection is no longer necessary.

The following information is required to log in via this extra connection.

1. The "public" IP address of the vtServer in the Cloud.
2. The port number to use for the extra connection.
3. The Private SSH key file with the correct SSH key.

The public IP address can be requested via the Cloud provider's Cloud interface.
Example Oracle:



Primary VNIC Information

Private IP Address: 10.0.0.40

Public IP Address: 132.145.169.211